Town of Arlington
Office of the Town Manager

Jim Feeney
Town Manager

730 Massachusetts Avenue
Arlington MA 02476-4908

To: Arlington Community
RE: Arlington is Victim of Cybercrime (BEC Attack)
Date: June 5, 2024

It is my unfortunate duty to report that the Town of Arlington has been a victim of cybercrime. Through what is known as a business email compromise (BEC), perpetrators used phishing, spoofing, social engineering, and compromised email accounts to ultimately facilitate wire fraud totaling $445,945.73. Most importantly, I want to assure the public that no sensitive or resident data was compromised. Below, I provide background on the crime and steps the Town is taking to recoup the loss and avoid future fraud.

We have been working with local and federal law enforcement and specialized consultants since we first became aware of the fraud. It is believed this BEC attack was perpetrated by an organization that is well resourced and located overseas. Here is what I am able to share. I have also provided an FAQ (frequently asked questions) at the end of this letter to provide additional details.

In September of 2023 Town employees received legitimate emails from a known vendor working on the Arlington High School Building Project to discuss issues with payment processing. Unbeknownst to the Town, threat actors had already compromised certain employee user accounts and were monitoring emails. They seized the opportunity to impersonate the vendor with an email domain that appeared genuine, requesting a change in their payment method from check to electronic funds transfer (EFT), a common method used by municipalities for on-going payments. The scam was aided by fabricating and subsequently deleting emails from employee accounts, as well as creating inbox rules to manage and hide incoming messages. Once the payment method was established, a series of four monthly payments were made. The monthly payments were diverted until the vendor reported not receiving payments in February 2024. It was immediately apparent that we had been defrauded, so we alerted law enforcement and our banking institution, began a digital forensics investigation, retained a breach coach, and instituted immediate response measures to secure our network. The investigation found that threat actor activity occurred in the Town's Microsoft environment between September 12, 2023 and January 30, 2024. It was also discovered there were other attempts to intercept wire payments totaling approximately

$5 million during this time period. Fortunately, these attempts were unsuccessful. It was further determined the threat actors had not infiltrated the network.

In the immediate aftermath of the scam the Town's Information Technology Department (IT) performed a force disconnection from the network, required a password change for all users, and enabled multi-factor authentication for key personnel. Unrelated to this incident, but due to an increase in phishing attempts, the IT Department had already begun to reconfigure email security settings in November to improve our email security. The Town reviewed other existing wire payments and also contracted a third-party auditor to bolster internal controls with a stricter policy related to wire transfer payments such as EFT and ACH (Automatic Clearing House).

As additional efforts to reduce the risk of falling victim to future cyberattacks, the Town has instituted mandatory cybersecurity training for all staff through the state's Municipal Cybersecurity Awareness Grant Program and has applied for additional state grant funding to be able to roll out multi-factor authentication for all staff. The Town was already in the process of rolling out an endpoint detection and response platform as part of the upcoming fiscal year. This platform will help prevent and detect malware, ransomware, and other advanced threats, providing security of critical systems and sensitive data.

With respect to the funds the Town was defrauded of, our banking institution was able to recover $3,308. The Town has since filed a claim with our insurer to hopefully further offset the loss. In the meantime, the vendor needed to be paid for services rendered over a four-month period, so at their June 4th meeting, the Arlington High School Building Committee voted to authorize payment to the vendor from the project funds. Any monies we recoup from this fraud will go back into this fund.

I want to emphasize that this loss does not negatively impact the completion of the High School Building project in any way.

In 2023 the FBI's Internet Crime Complaint Center received 21,489 BEC complaints with adjusted losses over $2.9 billion. It's a staggering number and a sobering reminder that malicious actors are common and during the course of this experience, I learned, well resourced. That being said, I want to you assure you that we are exhausting every avenue to recoup the funds that we were defrauded of, and we are making every effort to improve our cybersecurity posture. Cybersecurity is an ever-changing and evolving threat. As an organization we will continue to adapt our defenses to emerging threats through educating and training of our users, investing in the necessary tools moving forward, and establishing policies and protocols to protect our digital operations.

Sincerely,

Jim Feeney

Arlington Town Manager

Arlington BEC Attack Frequently Asked Questions

Money and Budget Impacts

Who is responsible for the money?
The Town of Arlington – specifically the AHS Building Project - is responsible for the $445,945.73 loss. The AHS Building Project funds have already been allocated and are separate from the Town of Arlington's annual operating budget.
The mechanism to pay the defrauded amount will be through the AHS Building Project fund. Fortunately, the AHS Building Project fund can cover the loss at this time and no aspects of the project will be altered or removed. The project schedule remains unchanged and is anticipated to be complete in the Fall of 2025. Visit ahsbuilding.org for more information on the AHS Building Project.

How does this impact the recent override and general budget?
As previously stated, the loss will be paid from the AHS Building project budget. Impacts to the general operating budget will come from investments in enhanced cybersecurity, which are outlined below under the question: "What is the Town doing now to avoid being a victim of another cyberattack?" Future investments will be considered through the Town's usual budgeting process.

Will our insurance cover any of these losses?
The Town has filed an insurance claim and hopes to recoup some money. Any funds recouped will go back into the AHS Building Project Fund.

Security and Incident

What immediate actions has the Town taken in response to this incident?

- Alerted law enforcement agencies and our banking institution.
- Began a digital forensics investigation and retained a breach coach.
- Instituted immediate response measures to secure our network.
- Completed an internal security audit of all transactions with this and other vendors.
- Completed a full reconciliation of the AHS building project budget.
- Began implementation of increased IT security measures (multi-factor for key personnel).
- Filed a claim with our insurance agency.

What is the Town doing now to avoid being a victim of another cyberattack?

- The Town has instituted mandatory cybersecurity training for all staff through the state's Municipal Cybersecurity Awareness Grant Program.
- In FY25 the Town will roll out a platform that continuously monitors end-user devices to detect and respond to ransomware and malware threats
- The Town has applied for state grant funding to be able to roll out multi-factor authentication for all staff.
- The Town will work with the Commonwealth to perform penetration testing.

- Cybersecurity is an ever-changing and evolving threat. As an organization we will continue to adapt our defenses to emerging threats through educating and training of our users, investing in the necessary tools moving forward, and establishing policies and protocols to protect our digital operations. Future cybersecurity investments will be considered through the Town's usual budgeting process.

Why did it take so long to discover the fraudulent activity?
Once the EFT payment method was established, monthly invoices continued to be successfully processed to the threat actors bank account. Legitimate payment confirmations were sent to the intended vendor, but it was not immediately evident that the payments were fraudulent.

Why did the Town wait so long to inform residents?
The matter was actively under investigation by law enforcement and our banking institution and could not be made public until these investigations were complete.

Is the Town confident that no other cyberthefts have occurred?
The investigation found that threat actor activity occurred in the Town's Microsoft environment between September 12, 2023 and January 30, 2024. During this time other attempts to intercept wire payments totaling approximately $5 million were discovered. Fortunately, these attempts were unsuccessful as the targets were well-established existing wires.

Was the vendor also compromised? What actions did they take following this incident?
No, the vendor was not compromised. They verified that all internal email and electronic files were secure. Additionally, they confirmed with all other vendors on the project that payments were secure. All vendors will notify if any payments are overdue.

What state and federal agencies were/are involved with the investigation?
The Town of Arlington immediately contacted local and federal law enforcement agencies, including the Federal Bureau of Investigations and Secret Service of the fraudulent payments, as soon as the fraud was discovered.

Is there support from the federal government to recoup these losses?
Unfortunately, cybercrimes of this nature are becoming more commonplace and the loss from this incident is lower than the minimum threshold considered for state or federal support. FDIC insurance does not protect accounts from fraud.

Why didn't Arlington's bank catch these fraudulent payments? And what is their liability, if any?
The bank likely would not realize these payments were fraudulent until they were notified, as the transactions were processed as a normal course of business. The transaction occurred between two legitimate domestic accounts, both originating and receiving, per instructions provided. Under current regulations, banks enjoy broad protections from liability resulting from wire fraud and their only duty is to their respective customers. According to the Federal Trade Commission, bank payment and transfer is the most prevalent payment method employed by fraudsters. As consumers

lose more and more to fraud each year, federal legislators have begun to push banks to do more to protect consumers from wire fraud. The Senate Committee on Banking, Housing and Urban Affairs is leading this effort.

Are we changing banks? If not, why?
At this time we do not feel compelled to change any of our banking institutions. These transactions could have occurred within any financial institutions without being flagged as problematic.

What other Massachusetts municipalities have been victims of cybercrime?
Since 2020, Tewksbury, Franklin, Quincy, Lowell, and Concord have all been victims of some form of cyberattack.